

OCA 87-1946

OFFICE OF CONGRESSIONAL AFFAIRS**Routing Slip**

	ACTION	INFO
1. D/OCA		X
2. DD/Legislation	XX	
3. DD/Senate Affairs		X
4. Ch/Senate Affairs		
5. DD/House Affairs		X
6. Ch/House Affairs		
7. Admin Officer		
8. Executive Officer		
9. FOIA Officer		
10. Constituent Inquiries Officer		
11. 		X
12. 		

SUSPENSE

11May87 (by: 3:00p.m.)
DateAction Officer:

Remarks:

Rec'd 11May87 at 12:20p.m.

No ~~action~~ relayed
to DMB 5/11/87
 ecf 11 May 87
 Name/Date

OCA 87-1945

OFFICE OF CONGRESSIONAL AFFAIRS**Routing Slip**

	ACTION	INFO
1. D/OCA		X
2. DD/Legislation	XX	
3. DD/Senate Affairs		X
4. Ch/Senate Affairs		
5. DD/House Affairs		X
6. Ch/House Affairs		
7. Admin Officer		
8. Executive Officer		
9. FOIA Officer		
10. Constituent Inquiries Officer		
11. [Redacted]		X
12.		

SUSPENSE 11 May 87 (by: 3:00p.m.)
Date

Action Officer:		
Remarks:		
Rec'd 11 May 87 at 12:20p.m.		

ecf 11 May 87

Name/Date



**EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503**

O/CONGRESSIONAL AFFAIRS
87-1946

May 11, 1987

SPECIAL

LEGISLATIVE REFERRAL MEMORANDUM

SPECIAL

TO: Legislative Liaison Officer

SEE ATTACHED DISTRIBUTION LIST

ON FILE Leg-
[illegible]

SUBJECT: NSC/OMB proposed report on H.R. 145 -- Computer Security Act as reported by two House Science and Technology subcommittees (a proposed markup is also attached.)

The Office of Management and Budget requests the views of your agency on the above subject before advising on its relationship to the program of the President, in accordance with OMB Circular A-19.

A response to this request for your views is needed no later than

3:00 p.m. -- MONDAY -- MAY 11, 1987

(Science and Technology Committee markup is May 13, 1987.)

Questions should be referred to Constance J. Bowers (395-3457), the legislative analyst in this office.


James C. Murr for
Assistant Director for
Legislative Reference

Enclosures

cc: Ed Springer	John Cooney	Bob Bedell
John Cunningham	Jack Carley	
Kevin Scheid	Greg Henry	

DISTRIBUTION LIST

<u>AGENCY</u>	<u>CONTACT</u>	<u>PHONE NUMBER</u>
Department of Commerce (04)	Mike Levitt	377-3151
Department of Defense (06)	Sam Brick	697-1305
Department of Energy (09)	Bob Rabben	586-6718
Department of Health and Human Services (14)	Frances White	245-7750
Department of Justice (17)	Jack Perkins	633-2113
Department of State (25)	Lee Howdershell	647-4463
Department of the Treasury (28)	Carole Toth	566-8523
Office of Personnel Management (22)	James Woodruff	632-5524
General Services Administration		
National Security Council		
Central Intelligence Agency		

Honorable Jack Brooks
Chairman, Committee on
Government Operations
U.S. House of Representatives
Washington, D.C. 20515

Dear Mr. Chairman:

I am pleased that through intensive consultations between the Administration and the Congress great progress has been made toward agreement on a Computer Security Act of 1987. I hope that this statement of Administration views will assist in offering constructive solutions to areas where further improvements are desirable.

As we have reviewed H.R. 145, a primary concern has been to assure that the roles of the National Bureau of Standards and the National Security Agency are discharged in a manner that will promote a sound public policy and result in efficient, cost effective, and productive solutions. In this regard it is the Administration's position that NBS, in developing Federal standards for the security of computers, shall draw upon technical security guidelines developed by NSA in so far as they are available and consistent with the requirements of civil departments and agencies to protect data processed in their systems. When developing technical security guidelines, NSA will consult with NBS to determine how its efforts can best support such requirements. We believe this would avoid costly duplication of effort.

Computer security standards, like other computer standards, will be developed in accordance with established NBS procedures. In this regard the technical security guidelines provided by NSA to NBS will be treated as advisory and subject to appropriate NBS review. In cases where civil agency needs will best be served by standards that are not consistent with NSA technical guidelines, the Secretary of Commerce will have authority to issue standards that best satisfy the agencies' needs. At the same time agencies will retain the option to ask for Presidential review of standards issued by the Department of Commerce which do not appear to be consistent with U.S. public interest, including that of our national security. I am enclosing proposed changes to the present text of H.R. 145 which are consistent with the NBS-NSA relationship outlined above and make several minor changes that would further improve the bill.

In closing, I want to assure you that a reported bill within the parameters outlined in this letter will have the Administration's support.

(To be signed by an appropriate
administration official.)

SACH145A

5/7/82

AMENDMENT IN THE NATURE OF A SUBSTITUTE
TO H.R. 145

OFFERED BY

Strike out all after the enacting clause and insert in
lieu thereof the following:

1 SECTION 1. SHORT TITLE.

2 This Act may be cited as the ``Computer Security Act of
3 1987``.

4 SEC. 2. PURPOSE.

5 (a) IN GENERAL.--The Congress declares that improving the
6 security and privacy of sensitive information in Federal
7 computer systems is in the public interest, and hereby
8 creates a means for establishing minimum acceptable security
9 practices for such systems, without limiting the scope of
10 security measures already planned or in use.

11 (b) SPECIFIC PURPOSES.--The purposes of this Act are--

12 (1) by amending the Act of March 3, 1901, to assign
13 to the National Bureau of Standards responsibility for
14 developing standards and guidelines for Federal computer
15 systems, including responsibility for developing
16 standards and guidelines needed to assure the
17 cost-effective security and privacy of sensitive
18 information in Federal computer systems, drawing on the

1 technical ^{guidelines} ~~advice~~ and assistance (including work products)
2 of the National Security Agency, ~~where appropriate~~

3 (2) to provide for promulgation of such standards and
4 guidelines by amending section 111(d) of the Federal
5 Property and Administrative Services Act of 1949;

6 (3) to require establishment of security plans by all
7 operators of Federal computer systems that contain
8 sensitive information; and

9 (4) to require mandatory periodic training for all
10 persons involved in management, use, or operation of
11 Federal computer systems that contain sensitive
12 information.

13 SEC. 3. ESTABLISHMENT OF COMPUTER STANDARDS PROGRAM.

14 The Act of March 3, 1901, (15 U.S.C. 271-278h), is
15 amended--

16 (1) in section 2(f), by striking out ``and`` at the
17 end of paragraph (18), by striking out the period at the
18 end of paragraph (19) and inserting in lieu thereof a
19 semicolon, and by inserting after such paragraph the
20 following:

21 `` (20) the study of computer systems (as that term is
22 defined in section 18(c) of this Act) and their use to
23 control machinery and processes. ``;

24 (2) by redesignating section 18 as section 20, and by
25 inserting after section 17 the following new sections:

1 "SEC. 18. (a) The National Bureau of Standards shall--

2 "(1) have the mission of developing standards,
3 guidelines, and associated methods and techniques for
4 computer systems;

5 "(2) except as described in paragraph (3) of this
6 subsection (relating to security standards), develop
7 uniform standards and guidelines for Federal computer
8 systems, except those systems excluded by section 2315 of
9 title 10, United States Code, or section 3502(2) of title
10 44, United States Code;

11 "(3) have responsibility within the Federal
12 Government for developing technical, management,
13 physical, and administrative standards and guidelines for
14 the cost-effective security and privacy of sensitive
15 information in Federal computer systems except--

16 "(A) those systems excluded by section 2315 of
17 title 10, United States Code, or section 3502(2) of
18 title 44, United States Code; and

19 "(B) those systems which are protected at all
20 times by procedures established for information which
21 has been specifically authorized under criteria
22 established by an Executive order or an Act of
23 Congress to be kept secret in the interest of
24 national defense or foreign policy,
25 the primary purpose of which standards and guidelines

CH145A

4

1 shall be to control loss and unauthorized modification or
2 disclosure of sensitive information in such systems and
3 to prevent computer-related fraud and misuse;

4 “(4) submit standards and guidelines developed
5 pursuant to paragraphs (2) and (3) of this subsection,
6 along with recommendations as to the extent to which
7 these should be made compulsory and binding, to the
8 Secretary of Commerce for promulgation under section
9 111(d) of the Federal Property and Administrative
10 Services Act of 1949;

11 “(5) develop guidelines for use by operators of
12 Federal computer systems that contain sensitive
13 information in training their employees in security
14 awareness and accepted security practice, as required by
15 section 5 of the Computer Security Act of 1987; and

16 “(6) develop validation procedures for, and evaluate
17 the effectiveness of, standards and guidelines developed
18 pursuant to paragraphs (1), (2), and (3) of this
19 subsection through research and liaison with other
20 government and private agencies.

21 “(b) In fulfilling subsection (a) of this section, the
22 National Bureau of Standards is authorized--

23 “(1) to assist the private sector, upon request, in
24 using and applying the results of the programs and
25 activities under this section;

1 “(2) to make recommendations, as appropriate, to the
2 Administrator of General Services on policies and
3 regulations proposed pursuant to section 111(d) of the
4 Federal Property and Administrative Services Act of 1949;

5 “(3) as requested, to provide to operators of
6 Federal computer systems technical assistance in
7 implementing the standards and guidelines promulgated
8 pursuant to section 111(d) of the Federal Property and
9 Administrative Services Act of 1949;

10 “(4) to assist, as appropriate, the Office of
11 Personnel Management in developing regulations pertaining
12 to training, as required by section 5 of the Computer
13 Security Act of 1987;

14 “(5) to perform research and to conduct studies, as
15 needed, to determine the nature and extent of the
16 vulnerabilities of, and to devise techniques for the cost
17 effective security and privacy of sensitive information
18 in Federal computer systems; and

19 “(6) to coordinate closely with other agencies and
20 offices (including, but not limited to, the Departments
21 of Defense and Energy, the National Security Agency, the
22 General Accounting Office, the Office of Technology
23 Assessment, and the Office of Management and Budget)--

24 “(A) to assure maximum use of all existing and
25 planned programs, materials, studies, and reports

145A

6

1 relating to computer systems security and privacy, in
 2 order to avoid unnecessary and costly duplication of
 3 effort; and

4 "(B) to assure, to the maximum extent feasible,
 5 that standards developed pursuant to subsection (a)
 6 (3) and (5) are consistent and compatible with
 7 standards and procedures developed for the protection
 8 of information in Federal computer systems which is
 9 authorized under criteria established by Executive
 10 order or an Act of Congress to be kept secret in the
 11 interest of national defense or foreign policy.

12 "(c) For the purposes of (1) developing/ ^{computer security technical} standards and
 13 guidelines under subsection (a)/ ^{(1) and} (3), and (2) performing
 14 research and conducting studies under subsection (b)(5), the
 15 National Bureau of Standards shall draw on the ^{guidelines,} technical/
 16 advice and assistance (including work products) of the
 17 National Security Agency, ~~where appropriate.~~

18 "(d) As used in this section--

19 "(1) the term 'computer system'--

20 "(A) means any equipment or interconnected
 21 system or subsystems of equipment that is used in the
 22 automatic acquisition, storage, manipulation,
 23 management, movement, control, display, switching,
 24 interchange, transmission, or reception, of data or
 25 information; and

1 “(B) includes--

2 “(i) computers;

3 “(ii) ancillary equipment;

4 “(iii) software, firmware, and similar
5 procedures;

6 “(iv) services, including support services;
7 and


8 “(v) related resources as defined by
9 regulations issued by the Administrator for
10 General Services pursuant to section 111 of the
11 Federal Property and Administrative Services Act
12 of 1949;

13 “(2) the term ‘Federal computer system’--

14 “(A) means a computer system operated by a
15 Federal agency or by a contractor of a Federal agency
16 or other organization that processes information
17 (using a computer system) on behalf of the Federal
18 Government to accomplish a Federal function; and

19 “(B) includes automatic data processing
20 equipment as that term is defined in section
21 111(a)(2) of the Federal Property and Administrative
22 Services Act of 1949;

23 “(3) the term ‘operator of a Federal computer
24 system’ means a Federal agency, ^{or} contractor of a Federal
25 agency ~~XXXXXX or other organization~~ that processes information



1 using a computer system on behalf of the Federal
2 Government to accomplish a Federal function;

3 - `` (4) the term 'sensitive information' means any
4 information, the loss, misuse, or unauthorized access to
5 or modification of which could adversely affect the
6 national interest or the conduct of Federal programs, or
7 the privacy to which individuals are entitled under
8 section 552a of title 5, United States Code (the Privacy
9 Act), but which has not been specifically authorized
10 under criteria established by an Executive order or an
11 Act of Congress to be kept secret in the interest of
12 national defense or foreign policy; and

13 - `` (5) the term 'Federal agency' has the meaning given
14 such term by section 3(b) of the Federal Property and
15 Administrative Services Act of 1949.

16 ``SEC. 19. (a) There is hereby established a Computer
17 System Security and Privacy Advisory Board within the
18 Department of Commerce. The Secretary of Commerce shall
19 appoint the chairman of the Board. The Board shall be
20 composed of twelve additional members appointed by the
21 Secretary of Commerce as follows:

22 - `` (1) four members from outside the Federal
23 Government who are eminent in the computer or
24 telecommunications industry, at least one of whom is
25 representative of small or medium sized companies in such

ACE145A

9

1 industry;

2 “(2) four members from outside the Federal
3 Government who are eminent in the fields of computer or
4 telecommunications technology, or related disciplines,
5 but who are not employed by or representative of a
6 producer of computer or telecommunications equipment; and

7 “(3) four members from the Federal Government who
8 have computer systems management experience, including
9 experience in computer systems security and privacy, at
10 least one of whom shall be from the National Security
11 Agency.

12 “(b) The duties of the Board shall be--

13 “(1) to identify emerging managerial, technical,
14 administrative, and physical safeguard issues relative to
15 computer systems security and privacy;

16 “(2) to advise the Bureau of Standards and the
17 Secretary of Commerce on security and privacy issues
18 pertaining to Federal computer systems; and

19 “(3) to report its findings to the Secretary of
20 Commerce, the Director of the Office of Management and
21 Budget, the Director of the National Security Agency, and
22 the appropriate Committees of the Congress.

23 “(c) The term of office of each member of the Board
24 shall be four years, except that--

25 “(1) of the initial members, three shall be

1 appointed for terms of one year, three shall be appointed
2 for terms of two years, three shall be appointed for
3 terms of three years, and three shall be appointed for
4 terms of four years; and

5 "(2) any member appointed to fill a vacancy in the
6 Board shall serve for the remainder of the term for which
7 his predecessor was appointed.

8 "(d) The Board shall not act in the absence of a quorum,
9 which shall consist of seven members.

10 "(e) Members of the Board, other than full-time
11 employees of the Federal Government, while attending meetings
12 of such committees or while otherwise performing duties at
13 the request of the Board Chairman while away from their homes
14 or a regular place of business, may be allowed travel
15 expenses in accordance with subchapter I of chapter 57 of
16 title 5, United States Code.

17 "(f) To provide the staff services necessary to assist
18 the Board in carrying out its functions, the Board may
19 utilize personnel from the National Bureau of Standards or
20 any other agency of the Federal Government with the consent
21 of the head of the agency.

22 "(g) As used in this section, the terms 'computer
23 system' and 'Federal computer system' have the meanings given
24 in section 18(c) of this Act."; and

25 (3) by adding at the end thereof the following new

1 section:

2 ``SEC. 21. This Act may be cited as the National Bureau
3 of Standards Act.'`.

4 SEC. 4. AMENDMENT TO BROOKS ACT.

5 Section 111(d) of the Federal Property and Administrative
6 Services Act of 1949 (40 U.S.C. 759(d)) is amended to read as
7 follows:

8 `` (d)(1) The Secretary of Commerce shall, on the basis of
9 standards and guidelines developed by the National Bureau of
10 Standards pursuant to section 18(a) (2) and (3) of the
11 National Bureau of Standards Act, promulgate standards and
12 guidelines pertaining to Federal computer systems, making
13 such standards compulsory and binding to the extent to which
14 the Secretary determines necessary to improve the efficiency
15 of operation or security and privacy of Federal computer
16 systems. The President may disapprove or modify such
17 standards and guidelines if he determines such action to be
18 in the public interest. The President's authority to
19 disapprove or modify such standards and guidelines may not be
20 delegated. Notice of such disapproval or modification shall
21 be submitted promptly to the Committee on Government
22 Operations of the House of Representatives and the Committee
23 on Governmental Affairs of the Senate and shall be published
24 promptly in the Federal Register. Upon receiving notice of
25 such disapproval or modification, the Secretary of Commerce

1 shall immediately rescind or modify such standards or
2 guidelines as directed by the President.

3 “(2) The head of a Federal agency may employ standards
4 for the cost effective security and privacy of sensitive
5 information in a Federal computer system within or under the
6 supervision of that agency that are more stringent than the
7 standards promulgated by the Secretary of Commerce, if such
8 standards contain, at a minimum, the provisions of those
9 applicable standards made compulsory and binding by the
10 Secretary of Commerce. ✓

11 “(3) The standards determined to be compulsory and
12 binding may be waived by the Secretary of Commerce in writing
13 upon a determination that compliance would adversely affect
14 the accomplishment of the mission of an operator of a Federal
15 computer system, or cause a major adverse financial impact on
16 the operator which is not offset by government-wide savings.
17 The Secretary may delegate to the head of one or more Federal
18 agencies authority to waive such standards to the extent to
19 which the Secretary determines such action to be necessary
20 and desirable to allow for timely and effective
21 implementation of Federal computer systems standards. The
22 head of such agency may redelegate such authority only to a
23 senior official designated pursuant to section 3506(b) of
24 title 44, United States Code. Notice of each such waiver and
25 delegation shall be transmitted promptly to the Committee on

(see insert p.17)

1 Government Operations of the House of Representatives and the
2 Committee on Governmental Affairs of the Senate and shall be
3 published promptly in the Federal Register.

4 `` (4) The Administrator shall revise the Federal
5 information resources management regulations (41 CFR ch. 201)
6 to be consistent with the standards and guidelines
7 promulgated by the Secretary of Commerce under this
8 subsection.

9 `` (5) As used in this subsection, the terms 'Federal
10 computer system' and 'operator of a Federal computer system'
11 have the meanings given in section 18(c) of the National
12 Bureau of Standards Act.``.

13 SEC. 5. TRAINING BY OPERATORS OF FEDERAL COMPUTER SYSTEMS.

14 (a) IN GENERAL.--Each operator of a Federal computer
15 system that contains sensitive information shall provide
16 mandatory periodic training in computer security awareness
17 and accepted computer security practice. Such training shall
18 be provided under the guidelines developed pursuant to
19 section 18(a)(5) of the National Bureau of Standards Act (as
20 added by section 3 of this Act), ^{for Federal civilian employees} and in accordance with the
21 regulations issued under subsection (c) of this section, for
22 all employees who are involved with the management, use, or
23 operation of computer systems.

24 (b) TRAINING OBJECTIVES.--Training under this section
25 shall be started within 60 days after the issuance of the

(see insert p.17)

14

1 regulations described in subsection (c). Such training shall
2 be designed--

3 (1) to enhance employees' awareness of the threats to
4 and vulnerability of computer systems; and

5 (2) to encourage the use of improved computer
6 security practices.

7 (c) REGULATIONS.--Within six months after the date of the
8 enactment of this Act, the Director of the Office of
9 Personnel Management shall issue regulations prescribing the
10 procedures and scope of the training to be provided ^{Federal civilian employees} under
11 subsection (a) and the manner in which such training is to be
12 carried out.

13 SEC. 6. ADDITIONAL RESPONSIBILITIES FOR COMPUTER SYSTEMS
14 SECURITY AND PRIVACY.

15 (a) IDENTIFICATION OF SYSTEMS THAT CONTAIN SENSITIVE
16 INFORMATION.--Within 6 months after the date of enactment of
17 this Act, each Federal agency shall identify each Federal
18 computer system, and system under development, which is
19 within or under the supervision of that agency and which
20 contains sensitive information.

21 (b) SECURITY PLAN.--Within one year after the date of
22 enactment of this Act, each such agency shall, consistent
23 with the standards, guidelines, policies, and regulations
24 prescribed pursuant to section 111(d) of the Federal Property
25 and Administrative Services Act of 1949, establish a plan for

.CE145A

15

1 the security and privacy of each Federal computer system
2 identified by that agency pursuant to subsection (a) that is
3 commensurate with/^{the risk and}the magnitude of the harm resulting from
4 the loss, misuse, or unauthorized access to or modification of
5 the information contained in such system. Copies of each such
6 plan shall be transmitted to the National Bureau of Standards
7 and the National Security Agency for advice and comment. A
8 summary of such plan shall be included in the agency's five-
9 year plan required by section 3505 of title 44, United States
10 Code. Such plan shall be subject to disapproval by the
11 Director of the Office of Management and Budget. Such plan
12 shall be revised annually as necessary.

13 SEC. 7. DEFINITIONS.

14 As used in this Act, the terms "computer system",
15 "Federal computer system", "operator of a Federal computer
16 system", "sensitive information", and "Federal agency"
17 have the meanings given in section 18(c) of the National
18 Bureau of Standards Act (as added by section 3 of this Act).

19 SEC. 8. RULES OF CONSTRUCTION OF ACT.

20 Nothing in this Act, or in any amendment made by this
21 Act, shall be construed--

22 (1) to constitute authority to withhold information
23 sought pursuant to section 552 of title 5, United States
24 Code; or

25 (2) to authorize any Federal agency to limit,

16

1 restrict, regulate, or control the collection,
2 maintenance, disclosure, use, transfer, or sale of any
3 information (regardless of the medium in which the
4 information may be maintained) that is--
5 (A) privately-owned information;
6 (B) disclosable under section 552 of title 5,
7 United States Code, or other law requiring or
8 authorizing the public disclosure of information; or
9 (C) public domain information.

(17)

Substitute language in place of para 4 page 13

The Administrator shall implement the standards issued by the Secretary of Commerce in the Federal Information Resources Management Regulation (41 CFR ch. 201), in accordance with subsection (a), section 206(a), and section 101(f).

Insert language between lines 10 and 11 page 12

When an agency provides a contract for the operation by a or on behalf of the agency of a computer system to accomplish an agency function, the agency shall, consistent with its authority, cause applicable computer security standards to be applied to such system.